IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH GOOGLE ACCOUNT GREGLXSTANG@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 2:25-mj-00103

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Garrett Q. Haws, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of

Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2023. I am currently assigned to the Office of the Resident Agent in Charge-HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents, I am familiar with child sexual abuse and exploitation investigations and their use of computers and other media devices.

3. Prior to my employment with HSI, I was a police officer with the Alexandria Police Department in Alexandria, Virginia, from January 2012 to March 2023. I received basic law enforcement training from the Northern Virginia Criminal Justice Training Academy in Reston, Virginia, and graduated in June 2012. I was a patrol officer and a detective during my tenure with the Alexandria Police Department. I received specialized training and investigated numerous criminal offenses. In March 2023, I was hired by HSI as a Special Agent. I received specialized training from the Federal Law Enforcement Training Center ("FLETC") in

Brunswick, Georgia. I graduated from the Criminal Investigator Training Program ("CITP") in July 2023 and HSI Special Agent Training ("SAT") in October 2023. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to 18 U.S.C. §§ 2251, 2252, and 2252A.

4. As a Special Agent, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, and everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography in the Southern District of West Virginia. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual

exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 (production of child pornography), 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2251 (production of child pornography) and 2252A (transportation, receipt, distribution, possession, and access with intent to view child pornography) (collectively, the "Subject Offenses") have been committed by Gregory Neal HAGER ("HAGER"). There is also probable cause to search the information described in Attachment A for the evidence, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the

United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

8. On November 26, 2023, Senior Trooper C.M. Riggleman ("Trooper Riggleman") with the West Virginia State Police ("WVSP") in Madison, Boone County, West Virginia, received a complaint about an inappropriate relationship between a 15-year-old minor female ("MV1") and an adult male. During the course of the investigation, Trooper Riggleman discovered photographs of HAGER's penis on MV1's cellphone. MV1 told Trooper Riggleman that HAGER had sent her the images on Snapchat, a social media application, and that she had been talking to HAGER via social media for approximately two years, since she was 13 years old. MV1 explained that she and HAGER had exchanged nude pictures and that HAGER had asked her for sexual intercourse.

9. Based on this information and Trooper Riggleman's knowledge about cellphones and other electronic devices and their use in criminal activity, Trooper Riggleman secured search warrants from a Boone County, West Virginia, Circuit Judge for HAGER's person and his residence on Riverside Drive in Madison, Boone County, West Virginia. The warrants authorized law enforcement to seize any electronic devices, among other items and information.

10. The search warrants were executed on December 7, 2023. On that date, law enforcement seized multiple electronic devices from HAGER's person and a vehicle he was riding in, as well as from his residence.

11. One of the devices seized from HAGER's residence was an external drive attached to a computer tower. A computer forensics examiner performed a "preview" of the external drive and discovered multiple images of MV1 that constituted child pornography as defined in 18 U.S.C. § 2256(8). In particular, some of the images depicted MV1 masturbating, and other images depicted MV1 displaying her nude body (and specifically, her pubic area) in a sexual manner.

12. Based on the device preview and the information described in paragraph 8 herein, Trooper Riggleman obtained a search warrant from a Boone County, West Virginia, Circuit Judge for the electronic devices that were seized on December 7, 2023.

13. An HSI forensic examiner reviewing the devices discovered that the external drive "previewed" during the execution of the search warrant at HAGER's residence contained nearly 300 images of MV1 that constituted child pornography as defined in 18 U.S.C. § 2256(8). At least some of the images appeared to be screenshots of a Snapchat video chat between MV1 and HAGER, during which MV1 was using her cellphone to film herself masturbating. Based on my training and experience, in order to

save those screenshots to the external drive, HAGER would have had to take them via the Snapchat application on his cellphone or on his computer and save them to either of those devices first.

14. The forensic examiner also discovered that HAGER utilized the Google Drive cloud storage associated with his Google account (i.e. the account described in Attachment A) to periodically back up photos saved on his cellphone and computer. Based on my training and experience, and my knowledge about the habits and characteristics of collectors of child pornography described herein, I know that Google Drive is a common method such collectors use to safeguard their collections of child pornography.

15. HSI sent a preservation letter to Google on April 10, 2025, requesting the preservation of all data related to the Google account described in Attachment A.

BACKGROUND CONCERNING GOOGLE[1]

16. Google is a United States company that offers to the public through its Google accounts a variety of online services,

---

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google account.

17. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google account when they first turn on the device, and a Google account is required for certain functionalities on these devices.

18. Signing up for a Google account automatically generates an email address at the domain "gmail.com." That email address will be the log-in username for access to the Google Account.

19. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition,

Google keeps certain records indicating ownership and usage of the Google account across services, described further after the description of services below.

20. Gmail: Google provides email services (called Gmail) to Google accounts through email addresses "@gmail.com" or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google account by the user. Google preserves emails associated with a Google account indefinitely, unless the user deletes them.

21. Contacts: Google provides an address book for Google accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicating with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

22. Messaging: Google provides several messaging services, including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

23. Google Drive: Google Drive is a cloud storage service automatically created for each Google account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a

record of who made changes and when changes were made to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them. Android device users can also use Google Drive to back up certain data from their devices. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

24. Photos: Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

25. Location History: Google collects and retains data about the location at which Google account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-

site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google account signed in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

26. Chrome and My Activity: Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google account in a record called My Activity. My Activity also collects and retains data about searches that users conduct within their own Google account or using the Google Search service while logged into their Google account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google account when the user is logged into their Google account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020,

unless the user deletes them or opts into automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

27. Google Play: Google accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

28. Google integrates its various services to make it easier for Google accounts to access the full Google suite of services. For example, users accessing their Google account through their browser can toggle between Google services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. And if a user logs into their Google account on the Chrome browser, their subsequent

Chrome browser and Google search activity is associated with that Google account, depending on user settings.

29. When individuals register with Google for a Google account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

30. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help

to identify which computers or other devices were used to access the Google account.

31. Google maintains the communications, files, and associated records for each service used by a Google account on servers under its control. Even after a user deletes a communication or file from their Google account, it may continue to be available on Google's servers for a certain period of time.

32. In my training and experience, evidence of who was using a Google account, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. For example, information from Gmail or Contacts can help to establish the identity of the person using the account; Google Play can identify apps that had been previously downloaded to the phone; Messaging may locate communications between the account owner and individuals with whom they are sharing relevant folders in Google Drive; and Location History can help to identify the user of the account by showing regular activity at their home or place of employment.

33. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and Internet searches are

often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation.

34. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crimes under investigation.

35. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses

under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

36. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators or potential victims. In addition, emails, instant messages, Internet activity, documents, and contact information can lead to the identification of co-conspirators, victims, and instrumentalities of the crimes under investigation.

37. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation, including, but not limited to, information that can be used to identify the account's user or users; the use of applications through which child pornography is stored, shared, or obtained; communications with minors for the purpose of producing child pornography or child erotica; and communication with other

individuals involved in the trafficking of child pornography materials.

CHARACTERISTICS OF PERSONS WHO COLLECT OR TRAFFIC CHILD PORNOGRAPHY

38. I have experience in assisting with, and leading, investigations into child pornography. I have conducted investigations into those who solicit and share child pornography by electronic means. I have worked with other law enforcement agencies to conduct investigations into those who solicit, share, and otherwise engage in activity related to child pornography.

39. As a result of the aforementioned knowledge and experience, I have learned that the characteristics described in this affidavit are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material may include, but is not limited to, photographs, negatives, slides, magazines, printed media, motion pictures, video tapes, books, and other media stored electronically on computers, digital devices, or related digital storage media.

40. Offenders who deal with the above-referenced child pornography material depicting minors engaged in sexually explicit conduct obtain or traffic in such materials through many sources

and by several methods and means. These sources, methods, and means include, but are not limited to, the following:

a. Downloading via the Internet and other computer networks (including from websites, peer-to-peer file-sharing networks, news groups, electronic bulletin boards, chat rooms, instant message conversations, internet relay chats, and e-mail).

b. Receiving from commercial sources within and outside of the United States through shipments, deliveries, and electronic transfer.

c. Trading with other persons with similar interests through electronic transfer, shipments, or deliveries.

41. These offenders collect materials depicting minors engaged in sexually explicit conduct for many reasons. These reasons include the following:

a. For sexual arousal and sexual gratification.

b. To facilitate sexual fantasies in the same manner that other persons utilize adult pornography.

c. As a medium of exchange in return for new images and video depicting minors engaged in sexually explicit conduct.

42. These offenders often view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Consequently, these offenders prefer not to

be without their child pornographic material for any prolonged period of time and often go to great lengths to conceal and protect their illicit collections from discovery, theft, or damage. To safeguard their illicit materials, these offenders may employ the following methods:

a. The use of Internet-based data storage services, such as Google Drive.

b. The use of labels containing false, misleading, or no titles.

c. The application of technologies, software and other electronic means such as encryption, steganography (the practice of concealing a file, message, image, or video within another file, message, image, or video), partitioned hard drives, and misleading or purposefully disguised applications on electronic devices.

d. The use of safes, safety deposit boxes, or other locked or concealed compartments within premises or structures that the offender controls.

CONCLUSION

43. For the reasons described herein, I believe there is probable cause to search the information described in Attachment A for the evidence, contraband, and/or fruits of the Subject Offenses further described in Attachment B. Based on the foregoing, I request that the Court issue the proposed search warrant.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Further your Affiant sayeth naught.

SPECIAL AGENT GARRETT Q. HAWS
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 15th day of May, 2025.

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA